CLAIMS

What is claimed is:

1. A data processing method for generating a digital signature, the method comprising the computer-implemented steps of:

receiving and transiently storing a first integer data value relating to a digital signature of an electronic message;

digitally computing a multiplicative inverse of the first integer data value modulo a prime modulus data value by computing a first quantity modulo the prime modulus data value;

wherein the first quantity substantially equals, modulo the prime modulus data value, the first integer data value raised to a power of a second quantity;

wherein the second quantity is two less than the prime modulus data value; and

storing the multiplicative inverse in a computer hardware storage element for use in determining the digital signature of the electronic message.

2. A method for generating a digital output signal indicating a multiplicative inverse of an integer data value modulo a prime modulus, the method comprising the steps of:

receiving a first signal, indicating a value of the integer data value, at a base input of a modulo exponentiation block of an electronic integrated circuit;

sending a second signal, indicating a value of the prime modulus, to a modulus input of the modulo exponentiation block; and

sending a third signal, indicating a value of the prime modulus less two, to an exponent input of the modulo exponentiation block;

wherein the modulo exponentiation block generates an output based on a first quantity modulo a value at the modulus input; and

wherein the first quantity substantially equals, modulo the value at the modulus input, a value at the base input raised to a power of a value at the exponent input.

3. A method for fabricating an electronic circuit that generates an output signal indicating a multiplicative inverse of an integer data value modulo a prime modulus, the method comprising the steps of:

connecting a first register holding signals indicating a value of the integer data value to a base input of a modulo exponentiation block;

connecting a second register holding signals indicating a value of the prime modulus, to a modulus input of the modulo exponentiation block;

connecting a third register holding signals indicating a value of the prime modulus less two, to an exponent input of the modulo exponentiation block;

wherein the modulo exponentiation block generates an output based on a first quantity modulo a value at the modulus input; and

wherein the first quantity substantially equals, modulo the value at the modulus input, a value at the base input raised to a power of a value at the exponent input.

4. An apparatus for generating an output signal indicating a multiplicative inverse of an integer modulo a prime modulus comprising:

a modulo exponentiation block configured to generate the output signal based on a first quantity modulo a value at a modulus input, the first quantity substantially equal, modulo the value at the modulus input, to a value at a base input raised to a power of a value at an exponent input;

a first input for receiving a first signal indicating a value of the integer, the first input connected to the base input;

a second input for receiving a second signal indicating a value of the prime modulus, the second input connected to the modulus input; and

a circuit connected to the second input configured to generate on a first output a third signal indicating a value of the prime modulus less two, the first output connected to the exponent input.

5. An apparatus for performing a particular operation for using digital signatures on a network, the apparatus comprising a modulo exponentiation block configured for producing a multiplicative inverse of an integer modulo a prime modulus.

6. The apparatus as recited in Claim 5, further comprising no circuitry block configured to perform an extended Euclidian algorithm (EEA) and no general-purpose processor configured by instructions to perform the EEA.

7. The apparatus as recited in Claim 5, wherein:

the particular operation is performed in a series of sequential computations accomplished over a corresponding series of computation cycles; and

the apparatus further comprises connections configured to use the modulo exponentiation block during a plurality of computation cycles of the series of computation cycles.

8. The apparatus as recited in Claim 5, wherein the particular operation is an RSA encrypting operation.

9. The apparatus as recited in Claim 5, wherein the particular operation is an RSA decrypting operation.

10. The apparatus as recited in Claim 5, wherein the particular operation is a digital signature algorithm signing operation.

11. The apparatus as recited in Claim 5, wherein the particular operation is a digital signature algorithm verifying operation.

12. A computer-readable medium carrying one or more sequences of instructions for generating a multiplicative inverse of an integer modulo a prime modulus, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

sending data indicating a value of the integer as an base input to a modulo exponentiation function;

sending data indicating a value of the prime modulus as an modulus input to the modulo exponentiation function; and

sending data indicating a value of the prime modulus less two as an exponent input of the modulo exponentiation function,

wherein

the modulo exponentiation function generates an output based on a first quantity modulo the modulus input, and

the first quantity substantially equals, modulo the modulus input, the base input raised to a power of the exponent input.

13. The computer-readable medium recited in Claim 12, wherein the exponentiation function sends the base input, the modulus input and the exponent input to a special-purpose block of circuitry configured to perform modulo exponentiation.